UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/763,621	04/26/2001	Harald Vater	JEK/YATER	8124

23364 7590 01/07/2005

BACON & THOMAS, PLLC
625 SLATERS LANE
FOURTH FLOOR
ALEXANDRIA, VA 22314

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 01/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Applicati n No.	Applicant(s)	
	09/763,621	VATER ET AL.	
	Examin r	Art Unit	
	Carl Colin	2136	

-- Th MAILING DATE of this communication appears on the cover sheet with th correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 September 2004* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 9/13/2004, Applicant amends claims 1, 3, 9, 11, and 12. Claims 1-18 are presented for examination.

2. Applicant's remarks, pages 9-10, filed on 9/13/2004, with respect to the objection of the specification and claims 3 and 11 have been fully considered and the objection has been withdrawn with respect to the amended specification and claims. With respect to claims 1 and 9 the rejection under 35 USC 101 has been withdrawn due to the amended claims.

2.1 Applicant's arguments, pages 11-14, filed on 9/13/2004, with respect to the rejection of claims 1-18 have been fully considered, but are moot in view of the new ground(s) of rejection. Applicant has amended the independent claims to further clarify the claimed invention. However, upon further consideration a new ground of rejection is made in view of Kocher.

Claim Objections

3. Claims 3 and 11 are objected to because it is not clear whether the claimed limitation refers to determination of only disguised input data is effected with with the aid of XOR operations, since determination of the disguised operation (h R_1) effected with the with the aid of XOR operations does hold true in yielding identical output data according to the example in the disclosure. Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4.1 **Claims 1-18** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Publication US 2001/0053220 to **Kocher et al**.

4.2 **As per claim 1**, **Kocher et al** discloses a data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation (h), the execution of the operation (h) requiring input data (x) and the execution of the operation (h) generating output data (y), characterized in that the operation (h) is disguised

before its execution, for example (see page 4, paragraph 0034), the disguised operation (h R_1) is executed with disguised input data (x O R_1) , for example (see page 4, paragraph 0034), and the disguising of the operation (h) and the input data (x) is coordinated such that the execution of the disguised operation (h R_1) with disguised input data (x O R_1) yields output data (y) identical with the output data (y) determined upon execution of the operation (h) with undisguised input data (x), whereby disguising operation (h) prevents analysis of said operation (h) and exposure of secret information about said semiconductor chip should a potential attacker intercept signal patterns generated during execution of said disguising operation (h R_1), for example (see page 4, paragraphs 0034-0036 and page 1, paragraph 0009).

As per claim 2, Kocher et al discloses the limitation of a data carrier characterized in that at least one random number (R_1) enters into the determination of the disguised operation (h R_1) and the disguised input data (x O R_1), for example (see page 4, paragraphs 0034-0035).

As per claim 3, Kocher et al discloses the limitation of a data carrier characterized in that the determination of the disguised operation (h R_1) and the disguised input data (x O R_1) is effected with the aid of XOR operations, for example (see page 4, paragraphs 0034-0035).

As per claim 4, Kocher et al discloses the limitation of a data carrier characterized in that the disguised operation (h R_1) is permanently stored in the data carrier in advance, for example (see page 2, paragraph 0011).

As per claim 5, Kocher et al discloses the limitation of a data carrier characterized in that at least two disguised operations (h R_1, h $R_{1'}$) are permanently stored in the data carrier in advance and one of the stored disguised operations (h R_1, h $R_{1'}$) is selected randomly when a disguised operation is to be executed, for example (see page 2, paragraphs 0011-0012 and page 6, paragraph 0059).

As per claim 6, Kocher et al discloses the limitation of a data carrier characterized in that the disguised operation (h R_1 is recalculated before its execution and the at least one random number (R_1) is redetermined for said calculation, for example (see page 7, paragraph 0069).

As per claim 7, Kocher et al discloses the limitation of a data carrier characterized in that the operation (h) is realized by a table stored in the data carrier which establishes an association between the input data (x) and the output data (y), for example (see page 2, paragraph 0011 and page 10, claim 37).

As per claim 8, Kocher et al discloses the limitation of a data carrier characterized in that the disguising of the input data (x) contained in the table is effected by combination with the at least one random number (R_1), for example (see page 10, claims 37 and 38).

Claim 9 is similar to claim 1 except for reciting that the disguised operation yields output data (y O R_2) which are disguised relative to the output data (y); and the output data can be determined from the disguised output data (y O R_2) with the aid of data (R2) used for disguising

the operation (h). **Kocher et al** discloses disguising the output data and the output data can be determined from the disguised output data (y O R_2) with the aid of data (R2) used for disguising the operation, for example (see page 7, paragraph 0068 and page 10, claims 37 and 38).

Claims 10-13 and 15-16 are similar to claims 2-5 and 6-7 respectively except for using a second random number, which is disclosed in the recitations above. **Kocher et al** also discloses using any combination of random numbers (see page 5, paragraph 0051).

As per claim 14, Kocher et al discloses the limitation of a data carrier characterized in that the random numbers (R_1R_2) for determining the first disguised operation (h R_1R_2) are inverse to the random numbers (R_1,R_2') for determining the second disguised operation (h R_1,R_2') with respect to the combination used for determining the disguised operations (h R_1R_2, h R_1,R_2'). **Kocher et al** discloses using two random numbers that can be the same or different, for example (see page 4, paragraph 0035).

As per claim 17, Kocher et al discloses the limitation of a data carrier characterized in that the disguising of the input data (x) contained in the table is effected by combination with the at least one random number (R_1) and the disguising of the output data (y) contained in the table is effected by combination with the at least one further random number (R_2), for example (see page 10, claims 37 and 38).

As per claim 18, Kocher et al discloses the limitation of a data carrier characterized in that the operation (h) is a nonlinear operation with respect to the combination used for disguising the operation (h), for example (see page 2, paragraph 0011 and page 10, claim 37).

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Carl Colin
Patent Examiner
December 30, 2004

EMMANUEL L. MOISE
PRIMARY EXAMINER